

Re: 09/343,823

REMARKS

As filed, this application contained claims 1-24. Claims 8-9 and 15-17 are cancelled in this amendment. New claims 25-32 are added in this amendment. Accordingly, claims 1-7, 10-14, and 18-32 are pending in this application.

The Examiner has rejected claims 1-5, 7-9, 18-21, and 23 under 35 U.S.C. § 102(e) as anticipated by Liao et al. U.S. Patent No. 6,292,833. The Examiner has rejected claims 6, 10-12, 14, 22, and 24 under 35 U.S.C. § 103(a) as obvious over the combination of Liao and Zicker U.S. Patent No. 5,862,475. The Examiner has rejected claim 13 under 35 U.S.C. § 103(a) as obvious over Liao. The prior art on which the Examiner has relied neither anticipates nor renders obvious applicants' claims, as currently presented. Accordingly, reconsideration is respectfully requested.

Claim 1 is amended herein to call for, *inter alia*:

a network element equipped with a processor for transmitting a message to the terminating system indicating that a transmission was received over a non-private link subject to unauthorized interception.

Liao does not teach or suggest a network element ... transmitting a message ... indicating that a transmission was received over a non-private link subject to unauthorized interception. Although Liao states that "connections may be made secure... through use of private networks", Liao conflates various methods of achieving secured connections, including private networks, encryption, and the use of other secure protocols such as SSL and secured HTTP. (Col. 9, lines 34-47.) Liao does not teach or suggest indicating that a transmission was received over a non-private link, and as best understood, does not teach or suggest any step of detecting or determining that a particular connection may use a non-private link. Accordingly, whether alone or in combination, Liao, and the other art on which the Examiner has relied, neither anticipates nor renders obvious applicants' amended claim 1.

Claim 4 is amended herein to herein to call for, *inter alia*, the step of:

responsive to determination that the route includes an insecure link, providing to said sender and prior to connection to said recipient an alert of the insecure nature of the transmission.

Re: 09/343,823

Liao does not teach or suggest the step of providing to the sender and prior to connection to the recipient an alert of the insecure nature of the transmission. Liao at most discloses setting or resetting a flag in a message transmitted to the mobile station (Col. 11, lines 16-22). Because the message is disclosed as transmitted **to the mobile station**, there is no mechanism to provide **to the sender** an alert of the insecure nature of the transmission. Moreover, Liao contains no motivation to modify the system of Liao to provide an alert to the sender, because Liao's disclosed system is directed to the problem of protecting a mobile device--i.e., a recipient--from unauthorized access to its local services provisioning data by a remote servers--i.e., a sender. In addition, since an attempt to access the mobile via an unsecured connection may arise from an unauthorized source, it would not be desirable in Liao's system to inform the source that such unsecured attempted access has been detected. Accordingly, whether alone or in combination, Liao, and the other art on which the Examiner has relied, neither anticipates nor renders obvious applicants' amended claim 4.

Claim 18 calls for:

18. A telecommunications system comprising:
means for interconnecting a caller to a called party; and
means for alerting the caller or called party when a call path is
established using at least one insecure link.

Liao does not teach or suggest means for alerting the caller or called party when a call path is established using at least one insecure link. Liao is directed to precluding unauthorized access to a mobile device's provisioning information, as opposed to protecting the security of an actual call. To the extent Liao may disclose setting a flag in a message transmitted to the mobile device, that message is used to gain access to or modify the mobile device's provisioning information. Thus, Liao does not disclose:

means for alerting a caller or called party;

means for determining that an insecure link is used to establish a call path; or

means for alerting in connection with the security status of an established a call path.

Accordingly, whether alone or in combination, Liao, and the other art on which the Examiner has relied, neither anticipates nor renders obvious applicants' claim 18.

Re: 09/343,823

New claim 25 calls for:

25. A method for providing secure transmissions in a telecommunications network comprising the steps of:
- a. establishing a route from a sender to a recipient;
 - b. determining whether at least a portion of the route includes a non-private link subject to unauthorized interception;
 - c. responsive to a positive result in said determining step, further determining whether a secure connection may be established between said sender and said recipient; and
 - d. responsive to a positive result in said determining step and a negative result in said further determining step, providing an alert of the insecure nature of the route.

As mentioned above in the remarks urging patentability of claim 1, Liao does not teach or suggest the step of determining whether at least a portion of the route includes a non-private link subject to unauthorized interception. In addition, Liao does not teach or suggest further determining whether a secure connection may be established between said sender and said recipient in response to having determined that a portion of a route includes a non-private link. Further, Liao does not teach or suggest providing an alert of the insecure nature of a route in response to determinations in the aforementioned two steps. Accordingly, whether alone or in combination, Liao, and the other art on which the Examiner has relied, neither anticipates nor renders obvious applicants' claim 25.

Claims 2-3 are dependent on claim 1; claims 5-7 and 10-14 are dependent on claim 4; claims 19-24 are dependent on claim 18; and claims 26-32 are dependent on claim 25. Accordingly each dependent claim is allowable for at least the same reasons as its respective parent claim. In addition, each dependent claim incorporates one or more additional structural or method-step limitations, which, in combination with the limitations of the respective parent claim, are novel and non-obvious over the prior art on which the Examiner has relied.

In particular, claim 13 calls for the additional step of issuing an alert when a previously secure route becomes insecure. Liao is silent with respect to the event of a previously secure route becoming insecure. Liao's Fig. 5 discloses making a determination of whether a "connection" is secure at one stage of a process. To the extent an alert may be issued in response to that determination, it is shown and described once, and any such alert would be issued without

Re: 09/343,823

regard to any previous state of the connection or route. Moreover, Liao does not disclose monitoring the connection such that subsequent changes in the security of the connection would be detected, or an alert responsively issued. Claim 13 is therefore patentable for these additional reasons.

As amended, all claims meet the formal requirements of 35 U.S.C. §112, and all claims are novel and nonobvious over the prior art on which the Examiner has relied in this application and in view of the general level of skill in the art. Accordingly, allowance of claims 1-7, 10-14, and 18-32 is respectfully solicited.

Respectfully Submitted,



Neil R. Ormos

Attorney for Applicant

Registration No. 35,309

Telephone: +1 630 979 2006

Dated: January 4, 2002

Re: 09/343,823

Version with Markings to Show Changes Made

1. (Amended) A telecommunications network comprising:

an originating system connected to a terminating system via at least one other network element; and

a network element equipped with a processor for transmitting a message to the terminating system indicating that a transmission was received over ~~an insecure link~~ a non-private link subject to unauthorized interception.

2. (Amended) The telecommunications network of claim 1 further comprising the terminating system alerting a called station ~~of the insecure nature of the~~ that said transmission was non-private upon receipt of the insecure ~~that said~~ said message.

3. (Amended) A telecommunications network of claim 1 further comprising the originating system alerting a calling party of ~~the insecure~~ presence of said non-private link.

4. (Amended) A method for providing secure transmissions in a telecommunications network comprising the steps of:

establishing a route from a sender to a recipient;

determining whether at least a portion of the route includes an insecure link; ~~and~~

~~providing an alert of the insecure nature of the transmission upon the~~ responsive to determination that the route includes an insecure link, providing to said sender and prior to connection to said recipient an alert of the insecure nature of the transmission.

5. The method of claim 4 further comprising the step of:

completing a call after the alert has been provided.

Re: 09/343,823

6. (Amended) The method of claim 4 wherein providing an alert includes issuing a distinctive ring at the recipient's station: a station associated with the recipient.

7. The method of claim 4 wherein providing an alert includes issuing a message on an identification display.

10. The method of claim 4 wherein providing an alert includes providing an audible voice message.

11. The method of claim 4 wherein providing an alert includes using an audible tone.

12. The method of claims 10 or 11 wherein providing an alert includes providing a periodic alert.

13. The method of claim 4 further comprising:

issuing an alert when a previously secure route becomes insecure.

14. The method of claim 4 wherein providing an alert includes a query screen on a personal computer.

18. A telecommunications system comprising:

means for interconnecting a caller to a called party; and

means for alerting the caller or called party when a call path is established using at least one insecure link.

Re: 09/343,823

19. The telecommunications system of claim 18 wherein the call path traverses a packet data network.

20. The telecommunications system of claim 18 further comprising means for determining whether an insecure link has been traversed.

21. The telecommunications system of claim 18 further comprising means for issuing insecure link alert signals to other elements in a telecommunications network.

22. The telecommunications system of claim 18 further comprising means for the caller and called party to hear insecure warning signals throughout the call.

23. The telecommunications system of claim 18 wherein the call path traverses a cell network.

24. The telecommunications system of claim 18 wherein the means for alerting is subject to parameters established for a particular subscriber.

25. A method for providing secure transmissions in a telecommunications network comprising the steps of:

a. establishing a route from a sender to a recipient;

b. determining whether at least a portion of the route includes a non-private link subject to unauthorized interception;

Re: 09/343,823

c. responsive to a positive result in said determining step, further determining whether a secure connection may be established between said sender and said recipient; and

d. responsive to a positive result in said determining step and a negative result in said further determining step, providing an alert of the insecure nature of the route.

26. The method of claim 25 wherein said telecommunications network includes at least one intermediate node in said route from said sender to said recipient, and wherein step c. thereof further comprises the step of:

transmitting a message including a security status request through each of said at least one intermediate node.

27. The method of claim 25 wherein said telecommunications network includes at least one intermediate node in said route from said sender to said recipient, and wherein step c. thereof further comprises the step of:

for each of said at least one intermediate node, if such node is insecure, receiving a message indicating such node is insecure.

28. The method of claim 25 further comprising the step of:

e. establishing a secure connection between said sender and said recipient.

29. The method of claim 25 further comprising the step of:

e. establishing a connection between said sender and said recipient despite a determination that a secure connection cannot be established.

Re: 09/343,823

30. The method of claim 25 wherein said alert is provided to a user of said sender, and further comprising the step of:

e. receiving authorization from said user, after said user has received said alert, to maintain a connection between said sender and said recipient.

31. The method of claim 25 wherein said alert is provided to a user of said recipient, and further comprising the step of:

e. receiving authorization from said user, after said user has received said alert, to establish a connection between said sender and said recipient.

32. The method of claim 25 further comprising the step of:

e. responsive to a positive result in said determining step and a negative result in said further determining step, establishing a new route between said sender and said recipient.